



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/462,616	04/03/2000	GUNTER MARINGER	0745/61002/N	5313

7590 10/06/2003

NORMAN H ZIVIN
COOPER & DUNHAM
1185 AVENUE OF THE AMERICAS
NEW YORK, NY 10036

EXAMINER

KLIMACH, PAULA W

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 10/06/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/462,616

Applicant(s)

MARINGER ET AL.

Examiner

Paula W Klimach

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 27/6/2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-14 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-14 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____
- 4) ☐ Interview Summary (PTO-413) Paper No(s). _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

Specification

Content of Specification

1.

- (a) Title of the Invention: See 37 CFR 1.72(a) and MPEP § 606. The title of the invention should be placed at the top of the first page of the specification unless the title is provided in an application data sheet. The title of the invention should be brief but technically accurate and descriptive, preferably from two to seven words may not contain more than 500 characters.
- (b) Cross-References to Related Applications: See 37 CFR 1.78 and MPEP § 201.11.
- (c) Statement Regarding Federally Sponsored Research and Development: See MPEP § 310.
- (d) Incorporation-By-Reference Of Material Submitted On a Compact Disc: The specification is required to include an incorporation-by-reference of electronic documents that are to become part of the permanent United States Patent and Trademark Office records in the file of a patent application. See 37 CFR 1.52(e) and MPEP § 608.05. Computer program listings (37 CFR 1.96(c)), "Sequence Listings" (37 CFR 1.821(c)), and tables having more than 50 pages of text were permitted as electronic documents on compact discs beginning on September 8, 2000.

Or alternatively, Reference to a "Microfiche Appendix": See MPEP § 608.05(a). "Microfiche Appendices" were accepted by the Office until March 1, 2001.

- (e) Background of the Invention: See MPEP § 608.01(c). The specification should set forth the Background of the Invention in two parts:
 - (1) Field of the Invention: A statement of the field of art to which the invention pertains. This statement may include a paraphrasing of the applicable U.S. patent classification definitions of the subject matter of the claimed invention. This item may also be titled "Technical Field."
 - (2) Description of the Related Art including information disclosed under 37 CFR 1.97 and 37 CFR 1.98: A description of the related art known to the applicant and including, if applicable, references to specific related art and problems involved in the prior art which are solved by the applicant's invention. This item may also be titled "Background Art."

- (f) Brief Summary of the Invention: See MPEP § 608.01(d). A brief summary or general statement of the invention as set forth in 37 CFR 1.73. The summary is separate and distinct from the abstract and is directed toward the invention rather than the disclosure as a whole. The summary may point out the advantages of the invention or how it solves problems previously existent in the prior art (and preferably indicated in the Background of the Invention). In chemical cases it should point out in general terms the utility of the invention. If possible, the nature and gist of the invention or the inventive concept should be set forth. Objects of the invention should be treated briefly and only to the extent that they contribute to an understanding of the invention.
- (g) Brief Description of the Several Views of the Drawing(s): See MPEP § 608.01(f). A reference to and brief description of the drawing(s) as set forth in 37 CFR 1.74.
- (h) Detailed Description of the Invention: See MPEP § 608.01(g). A description of the preferred embodiment(s) of the invention as required in 37 CFR 1.71. The description should be as short and specific as is necessary to describe the invention adequately and accurately. Where elements or groups of elements, compounds, and processes, which are conventional and generally widely known in the field of the invention described and their exact nature or type is not necessary for an understanding and use of the invention by a person skilled in the art, they should not be described in detail. However, where particularly complicated subject matter is involved or where the elements, compounds, or processes may not be commonly or widely known in the field, the specification should refer to another patent or readily available publication which adequately describes the subject matter.
- (i) Claim or Claims: See 37 CFR 1.75 and MPEP § 608.01(m). The claim or claims must commence on separate sheet or electronic page (37 CFR 1.52(b)(3)). Where a claim sets forth a plurality of elements or steps, each element or step of the claim should be separated by a line indentation. There may be plural indentations to further segregate subcombinations or related steps. See 37 CFR 1.75 and MPEP § 608.01(i)-(p).
- (j) Abstract of the Disclosure: See MPEP § 608.01(f). A brief narrative of the disclosure as a whole in a single paragraph of 150 words or less commencing on a separate sheet following the claims. In an international application which has entered the national stage (37 CFR 1.491(b)), the applicant need not submit an abstract commencing on a separate sheet if an abstract was published with the international application under PCT Article 21. The abstract that appears on the cover page of the pamphlet published by the International Bureau (IB) of the World Intellectual Property Organization (WIPO) is the abstract that will be used by the USPTO. See MPEP § 1893.03(e).

- (k) Sequence Listing. See 37 CFR 1.821-1.825 and MPEP §§ 2421-2431. The requirement for a sequence listing applies to all sequences disclosed in a given application, whether the sequences are claimed or not. See MPEP § 2421.02.
2. This application does not contain an abstract of the disclosure as required by 37 CFR 1.72(b). An abstract on a separate sheet is required.

Claim Rejections - 35 USC § 112

3. **Claim 3** rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 3 recites the limitation "...the first response (Response 2)..." in claim 3 lines 2-3. There is insufficient antecedent basis for this limitation in the claim. The examiner believes that this may be a typo and should read "... the second response (Response 2)."

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. **Claim 1** is rejected under 35 U.S.C. 102(e) as being anticipated by Brown (5,740,361).

Brown suggests a method for mutual authentication of components in a network using the challenge-response method (Fig. 2 and 3), in which, in order to authenticate a terminal (M), in particular a mobile station, with the network, the network (N) uses a request to request from an authentication center (AUC) (Brown's Authentication Deity) at least one data pair comprising a

Art Unit: 2131

first random number (Challenge 1) and a first response (Response 1) (part 72 of Figure 2), and passes the first random number (Challenge 1) to the terminal (M) (part 80 Challenge Cs of Figure 3) which uses an internally stored key (Ki) likewise to calculate from this the first response (Response 1) and sends this to the network (N) (part 84 Response Ru of Figure 3), in which case, furthermore, the network (N) is authenticated with the terminal (M) in that the terminal sends a second random number (Challenge 2) to the network (part 82 challenge Cu of figure 3), to which the network responds with a second response (Response 2) calculated in the AUC (part 86 Response Rs of figure 3), wherein the first response (Response 1) sent from the terminal (M) to the network (N) is at the same time used as the second random number (Challenge 2), in which case the network has already requested the second response (Response 2) from the AUC in advance, together with the first random number and the first response, as part of a triplet data set (Challenge 1/R.esponse 1/Response 2) (Figure 2).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. **Claims 2-14** are rejected under 35 U.S.C. 103(a) as being unpatentable over Brown as applied to claim 1 above, and further in view of Tsubakiyama (5,544,245).

8. *In reference to claims 2 and 7*, Brown does not expressly disclose a method wherein the second random number (Challenge 2) is an interpretation of the first message sent by the terminal.

Tsubakiyama suggests a method (Fig. 2) where the message sent from the network N (C1) is used as a challenge to the user named i who interprets the challenge and responds to the challenge with the response C2

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the response given by the terminal in the system of Brown as the challenge as in the method of Tsubakiyama. One of ordinary skill in the art would have been motivated to do this because it would provide a mutual authentication which enables the network and each user to authenticate each other without inviting the chosen plaintext attack and the known plaintext attack on the encryption algorithm in the authentication protocol and permits the deliver of a key for cipher communication without the need of increasing the amount of data to be transmitted for the protocol for mutual authentication between the network and each user (Tsubakiyama column 2 lines 36-46).

9. *In reference to claim 3*, wherein the first random number (Challenge 1) and the second response (Response 2) are transmitted from the network (N) to the terminal (M) immediately successively in time. Fig. 3 in the system described by Brown the challenge and response are relatively successively carried out.

10. *In reference to claim 4*, wherein the data pair (Challenge 1/Response 2) is transmitted from the network (N) to the terminal (M) simultaneously, in the form of a single data set. The make up of the data set is a design choice.

11. *In reference to claims 5 and 6*, wherein the network requests data sets from the authentication center (AUC) in the form of triplet data sets (Challenge 1/Response 1/Response 2). Figure 2 of Brown discloses a system where the Challenge and response is sent to the Authentication Deity in one message, which that Authentication Deity responds to in the affirmative or in the negative which suggests that the values are sent to the Service because when the Authentication Deity replies it indicates that the two systems either have the same copy of the challenge and response or not.
12. *In reference to claims 8-10*, wherein the filling out process is carried out on a subscriber-specific basis, and wherein the complete length of the first response (Response 1) is shortened before transmission to the other station. Tsubakiyama discloses the manipulation of the data sent to the subscriber (user) to create a key (column 5 lines 12-15).
13. *In reference to claim 11*, wherein the network is a GSM network. Brown discloses the network being composing of a global computer network and therefore the possibility of it being a GSM network (column 6 lines 26-27).
14. *In reference to claim 12*, wherein the network is a wire-based network. Brown also discloses another embodiment of the invention may be small domestic networks and therefore wire-based networks (column 6 lines 27-29).
15. *In reference to claim 13*, wherein the individual, mutually authenticating components in a wire-based network are different monitoring units of computers which authenticate themselves with a central computer, and vice versa (figure 1).
16. *In reference to claim 14*, wherein the AUC calculates the triplet data sets requested by the network and transmits these to the network off-line and independently of time, on request by the

Art Unit: 2131

network, but in any case before the data interchange between the network and the terminal. The data sent from the Authentication Deity, in the system disclosed by Brown, is sent before the reauthentication (column 9 line 66 to column 10 line 5).

Conclusion

17. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Tsubakiyama	5,544,245
Brown	5,740,361

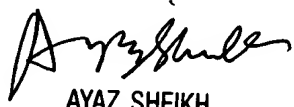
18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (703) 305-8421.

The examiner can normally be reached on Mon to Fri 7:15 a.m to 3:45 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-4832.

PWK


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGICAL CENTER 2100